INFO-HAMS Digest  Sun, 17 Dec 89  Volume 89 : Issue 1033

Today's Topics:



---

Date: Sun, 17 Dec 89 14:06:20 MST
From: jimkirk@CORRAL.UWyo.Edu (James Kirkpatrick)
Subject: Cellular Encryption
Message-ID: <891217140620.20200730@UWYO.BITNET>

Dube Todd writes --

>Are you telling me that every person who has a phone can then communicate with
>ANYONE else who has a phone, safe in the knowledge that NO ONE else can decode
>and thus monitor his conversation?
>I'll eat my posting when you tell me how this is done, John.

For an excellent overview of how this sort of thing is done, CURRENTLY, I suggest the May 1988 issue of the Proceedings of the IEEE. Any University library should have back issues, I'm certain they should be hanging around TI (where Dube apparently works) as well as better public libraries. In particular, Whitfield Diffie's article The First Ten Years of Public-Key Cryptography, which explains how the Motorola STU-III secure telephone works, as well as other devices and concepts.

If you accept that DES is "secure enough", as an example, the only real problems are transmission of digital data over a voice link at an acceptably high rate for human speech, and exchanging the DES keys. The details of secure key exchange, even in plain view of an eavesdropper, have been solved in several different ways. See the article for details.

It does require a different telephone than you've got, mainly in that you need D/A and A/D conversion, high-speed modems, DES chips, and a few other "smarts", but it is in current operation in the government arena. Has been for several years. And digital cellular will already have just about all that's required.

Bon apetite!

---

Date: 17 Dec 89 22:21:29 GMT

From: tank!jill@handies.ucar.edu  (jill holly hansen)
Subject: FT-470, the continuing saga...
Message-ID: <6778@tank.uchicago.edu>

In article <25897B37.3442@paris.ics.uci.edu>
     Clark Turner <turner@ics.uci.edu> writes:

:The Yaesu engineer at Cerritos which I spoke to said that such a change was
:UNLIKELY to help in the general case.  He said that the "fix" was used for
:some specific problems that occurred out in Illinois (somewhere in the
                                                        ^^^^^^^^^^^^^^^^
:midwest) where the IF was under direct attack by a local 2KW repeater signal.
 ^^^^^^
:----------
:Clark S. Turner                        "When the going gets weird,
:WA3JPG                                  the weird turn pro."
:turner@ics.uci.edu                     -Hunter Thompson
:----------

Clark, you can find Illinois on a good map just to the east of Iowa.

------------------------------

Date: 17 Dec 89 17:16:49 GMT
From: ccncsu!handel.CS.ColoState.Edu!wendt@boulder.colorado.edu  (alan l wendt)
Subject: Interception of E-Mail by spies
Message-ID: <3497@ccncsu.ColoState.EDU>

In article <17453@rpp386.cactus.org> jeremy@rpp386.UUCP (Jeremy S. Anderson)
writes:
>
>    E-mail privacy rights (and the right against your data transmissions
>being tapped) are very shaky legal ground.  It is legal to mail encrypted
>messages.  The crypt(1) function under UNIX is a childishly easy cipher to
>break with the proper tools.  The crypt(3) library routine uses DES, which is
>a little more sophisticated.  This cipher was developed by the NSA.  I
>don't personally know how to break it, nor does anyone I have asked about it.
>With sufficient brute-force application (i.e. 6 or 7 Cray-hours) I understand
>it is breakable.  There is a rumor that combining these two encryption
>methods carefully will produce a very strong cipher.  Perhaps an unbreakable
>one.  This is a difficult area to provide hard facts on.  Most serious
>professional cryptographers are either in corporate think-tanks or are with
>the NSA.  Both groups usually have very heavy secrecy agreements over their
>heads, which makes it difficult for me to locate qualified people to quiz
>on this subject.
>
I'm not a cryptologist.  It seems to me that the first thing to do before
encrypting the message is to LZW-compress it.  This does three things:

1. Removes redundancy. Some attacks work on repeated phrases, letter
   frequencies, etc, and this eliminates all such. The output of a
   good compression algorithm will resemble random noise, because it
   uses the information conduit most effectively.

2. Breaks the 8-bit chunking. This forces the decoder to consider
   decodings that span characters, making the job somewhat harder.

3. The reason to use LZW instead of Huffman is that an error in an
   LZW transmission tends to render the rest of the message garbage,
   while errors in Huffman transmissions (especially with fixed
   tables) do not. This makes it necessary to decode the message
   from left to right.

If you use the standard "compress" program, strip off any magic numbers
or other common sequence that it may place at the front of the message.
You do NOT want the message to begin with a known sequence. This
applies to any common sequence that compress might begin each message with.
Strip it off and replace it later. Turing's job was made easier because
the Germans usually began each message with the date (or something).

These precautions followed with DES encoding should push the cost
of decoding your message far beyond anything the NSA can afford
to do to megabytes of traffic per day.

I'm posting this as a followup to the article in misc.legal.
These points may have been covered many times in sci.crypt
but I don't read that.

Alan Wendt

---

Date: 17 Dec 89 16:11:10 GMT
From: cs.utexas.edu!asuvax!anasaz!john@tut.cis.ohio-state.edu (John Moore)
Subject: pudgy wound helical antenna (60m vertical in my living room!)
Message-ID: <1047@anasaz.UUCP>

In article <1260012@hpmwtlb.HP.COM> timb@hpmwtd.HP.COM (Tim Bagwell) writes:
]2) I can appreciate the space saving aspect of the design, but you get what
]   you pay for. I don't think you can do better than a full length antenna.
]   To capture the most energy you need as large an effective aperture as you
]   can get. However, I have no doubt that you can do better than your window
]   antenna (which, I admit, do work remarkably well).

I would like to dispell a widely held misconception here. While aperture

is important, what counts is EFFECTIVE aperture, not physical
aperture. A traveling wave cannot distinguish dimensions much smaller
than its wavelength. Hence, a magnetic dipole on a 6" loopstick is, in
theory, about as effective as a physical dipole (I don't have the exact
numbers here). A physical antenna that approaches a wavelength or
more in size starts to exhibit aperture related to its size. Smaller
antennas have effective apertures unrelated to their size.

Small antennas do have the following problems:

(1) Larger losses in impedance matching due to the large inductances
    required. These can be VERY significant. Note that a magnetic
    dipole (such as a loopstick) has these losses in both the matching
    network and the antenna itself.
(2) Very narrow bandwidth OR very complex impedance matching OR
    very high loss. You can't broaden the bandwidth without either
    screwing up the match or de-Q'ing the antenna through IR losses.
(3) Lousy directivity. A magnetic antenna has a dipole pattern. I would
    point out, however, that while a loopstick is not very directional,
    it has a VERY sharp null and makes a very good DF antenna on HF.

--
John Moore (NJ7E)           mcdphx!anasaz!john asuvax!anasaz!john
(602) 861-7607 (day or eve) long palladium, short petroleum
7525 Clearwater Pkwy, Scottsdale, AZ 85253
Freedom and Communism are incompatable.

------------------------------

Date: 17 Dec 89 20:52:06 GMT
From: mvac23!thomas@louie.udel.edu  (Thomas Lapp)
Subject: Transmitter found?
Message-ID: <129.UUL1.3#5131@mvac23.UUCP>

(mail direct to user failed with unknown PID in alias for the username)
Whilst driving on Interstate 70 over Thanksgiving, I passed a TIS
which was advertised just before getting to a particular rest stop.

According to my map, the rest stop is shown between exits 35 and 42, and
is located near Myersville, MD.  It is between Fredrick and Hagerstown
Maryland.  Might this be the "unknown" station below (it broadcasts on 530,
but I didn't listen for call -- maybe next week when I again pass that way...):

> MD: TIS, location unknown
>                       [MD]_____________    0.5300____KNJX865   (govt recds)
>               "         "                  1.6100____KNJX865   (govt recds)
> MD: TIS, xmtr located at Rt 70 and Rt 695, Baltimore
>                       [Baltimore, MD]_____    0.5300____WNAL785   (govt recds)

- tom

--
internet     : mvac23!thomas@udel.edu  or  thomas%mvac23@udel.edu
uucp         : {ucbvax,mcvax,psuvax1,uunet}!udel!mvac23!thomas
Europe Bitnet: THOMAS1@GRATHUN1
Location: Newark, DE, USA
Quote   : Virtual Address eXtension.  Is that like a 9-digit zip code?

--
The UUCP Mailer

------------------------------

End of INFO-HAMS Digest V89 Issue #1033
**************************************